IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: :

    Shiho Moriai et al. :

Serial No.: To be assigned : Art Unit: To be assigned

Filed: Herewith : Examiner: To be assigned

For: APPARATUS AND METHOD FOR : Atty Docket: 0162/00547
     EVALUATING RANDOMNESS OF
     FUNCTIONS, RANDOM FUNCTION :
     GENERATING APPARATUS AND
     METHOD, AND RECORDING :
     MEDIUM HAVING RECORDED
     THEREON PROGRAMS FOR :
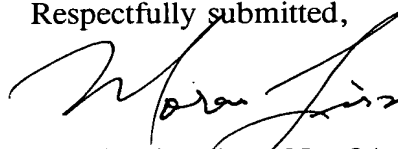   IMPLEMENTING THE METHODS

INFORMATION DISCLOSURE STATEMENT

Assistant Commissioner for Patents
Washington, D.C.   20231

Sir:

       For insuring compliance with the applicant's duty of disclosure under 37

CFR § 1.56, the undersigned hereby submits the documents listed on the attached

Form PTO-1449 for consideration by the Examiner in charge of the above-identified

patent application. The relevance of the references is indicated on the enclosed copy of

the International Search Report. It is respectfully requested that the Examiner initial

and return a copy of the enclosed PTO-1449, and indicate in the official file wrapper

of this patent application that the documents have been considered.

                 Respectfully submitted,

                 Morris Liss, Reg. No. 24,510
                 Pollock, Vande Sande & Amernick, R.L.L.P.
                 1990 M Street, N.W.
                 Washington, D.C. 20036-3425
                 Telephone: 202-331-7111

Date: 2/2/00

FORM PTO-1449

INFORMATION DISCLOSURE CITATION

Atty Docket 162/547	Serial No. 09/463907 To be assigned
Applicant 420 Rec'd PCT/PTO 0 2 FEB 2000 Shiho Moriai et al.	
Filing Date Herewith	Group Art Unit To be assigned

U.S. PATENT DOCUMENTS

Examiner Initial		Document Number	Date	Name	Class	Sub-Class	Filing Date
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						

FOREIGN PATENT DOCUMENTS

		Document Number	Date	Country	Class	Sub-Class	Trans-lation
	AL						Yes No
	AM						Yes No

OTHER (Including Author, Title, Date, Pertinent Pages, etc.)

	AN		Shiho Moriai, "How to Design Secure S-boxes against Differential, Linear, Higher Order Differential, and Interpolation Attacks," Telecommunications Advancement Organization of Japan, SCIS '98, 2.2C, January 1998, pp.1-8
	AO		Hamade, Takeshi, et al., "On Partitioning Cryptanalysis of DES," Telecommunications Advancement Organization of Japan, SCIS '98, 2.2A, January 1998, pp. 1-8
	AP		Langford, S.K., and Hellman, M.E., "Differential-Linear Cryptanalysis," Lecture Notes in Computer Science, Advances in Cryptology CRYPTO '94, Vol. 839, 1994, pp. 17-25
	AQ		Sakurai, Kouichi, "Angou riron no kiso," Kyoritsu Shuppan, pp. 69-72, 1996
	AR		Kanda, Masayuki, et al., "A Round Function Structure Consisting of Few S-boxes (Part II)," Telecommunications Advancement Organization of Japan, SCIS '98, 2.2.D, January 1998, pp. 1-8
	AS		Moriai, Shiho, et al., "S-box Design Considering the Security Against Known Attacks on Block Ciphers," Technical Report of the IEICE, ISEC98-13, Vol. 98, NO. 227, 30 July 1998, pp. 25-32

Examiner	Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP § 609.
Draw line through citation if not in conformance and not considered.
Include copy of this form with next communication to Applicant.